

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA,

Criminal No. 16-317 (JRT/FLN)

Plaintiff,

v.

TERRY LEE CARLSON, SR.

**MEMORANDUM OPINION
AND ORDER ON REPORT AND
RECOMMENDATION OF
MAGISTRATE JUDGE**

Defendant.

Carol M. Kayser, Assistant United States Attorney, **OFFICE OF THE
UNITED STATES ATTORNEY**, 404 United States Courthouse, 316
North Robert Street, St. Paul, MN 55101, for plaintiff.

Lee R. Johnson, **JOHNSON & GREENBERG PLLP**, 1660 South
Highway 100, Suite 500, St. Louis Park, MN 55416, for defendant.

This case resulted from a 2015 FBI investigation into a website that facilitated the distribution of child pornography available on a hidden network designed to shroud users with anonymity. The FBI commenced the investigation pursuant to a warrant issued by a magistrate judge sitting in the Eastern District of Virginia (the “Authorizing Judge”). On February 8, 2017, Defendant Terry Lee Carlson, Sr. moved to suppress evidence and statements obtained through the FBI investigation. On March 23, 2017, United States Magistrate Judge Franklin Noel (the “Magistrate Judge”) issued a Report and Recommendation (“R&R”) recommending that the Court grant Carlson’s motion to suppress evidence obtained as a result of the FBI investigation and grant in part and deny

in part Carlson's motion to suppress statements that he made to the FBI. On April 24, 2017, the government filed several objections to the R&R.

This case implicates novel issues involving sophisticated technology and the scope of the Fourth Amendment. The underlying FBI investigation has resulted in numerous district courts addressing the very same issues in this case – the validity of the warrant issued in the Eastern District of Virginia and the admissibility of evidence obtained under that warrant. Most courts have denied motions to suppress evidence obtained as a result of the warrant, but have applied varying approaches.

On July 24, 2017, the Eighth Circuit issued its decision in *United States v. Horton*, No. 16-3976, 2017 WL 3122073 (8th Cir. July 24, 2017), which reversed a ruling by the District Court for the Southern District of Iowa to suppress evidence discovered under the same warrant at issue in this case. The Court has considered these new developments in the law, the well-reasoned R&R, and the parties' thorough and well-written briefings. Because the *Horton* decision addressed the same warrant and held that the *Leon*¹ good-faith exception to the exclusionary rule of evidence applies (see 2017 WL 3122073, at *7), the Court will deny Carlson's motions to suppress statements and evidence law enforcement obtained as a result of the warrant, sustain the government's objections, and adopt the R&R to the extent it denies Carlson's motion to suppress.

¹ *United States v Leon*, 468 U.S. 897 (1984).

FACTUAL BACKGROUND²

I. THE FBI INVESTIGATION OF PLAYPEN

Since approximately August 2014, a website called “Playpen”³ operated on the anonymous “Tor” network, sometimes called the “dark web,” which is a network that “protects users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user.” (Gov’t’s Resp. to Def.’s Mem. in Supp. of Mot. to Suppress (“Gov’t’s Resp.”), Ex. 1 at 3-33 (“Macfarlane Aff.”), ¶¶ 7-8, 11, Jan. 31, 2017, Docket No. 25.) Because communications on the Tor network are routed to obscure a user’s true location, “[t]here is no practical way to trace the user’s actual IP.” (*Id.* ¶ 8.)

A user could only access Playpen if the user connected to the Tor network, knew the hidden Playpen web address,⁴ and entered a Playpen username and password. (*Id.* ¶¶ 10, 12, 14.) Playpen instructed its visitors “not [to] post information here that can be

² The factual details of this investigation are not in dispute. The factual information summarized here has been drawn from the FBI’s warrant applications, including attachments and accompanying affidavits, (*see* Gov’t’s Resp., Exs. 1-2, Jan. 31, 2017, Docket No. 25), as well as statements made at a hearing on February 8, 2017 (Tr. of Mot. Hr’g, Feb. 13, 2017, Docket No. 33).

³ Agent Macfarlane’s affidavit refers to the website at issue as the “TARGET WEBSITE.” (*See* Macfarlane Aff. ¶ 2.) The government was concerned about disclosing the website’s name because the website was active at the time the government submitted the warrant application. (*Id.* ¶ 2 n.1.) The government has since disclosed that “Playpen” is the website at issue. (*See* Gov’t’s Objs. to R&R at 10-11 n.5, Apr. 24, 2017, Docket No. 51.)

⁴ Because Playpen was a hidden website, one could not simply perform a Google-type search to locate it; instead, Playpen users needed to obtain the specific web address from other users or websites. (Macfarlane Aff. ¶ 10.)

used to identify you” and that “[t]his website is not able to see your IP and can not [sic] collect or send any other form of information to your computer except what you expressly upload.” (*Id.* ¶ 13.)

Once logged into Playpen, users could access a number of forums and topics where they could upload, view, and discuss child pornography. (*Id.* ¶¶ 14, 16-18.) The images and videos shared through the website were categorized according to victim age, gender, and type of sexual activity. (*Id.* ¶¶ 14-18.) Playpen also contained certain features such as private messaging and file hosting that facilitated the distribution of child pornography. (*Id.* ¶¶ 20-25.) On February 19, 2015, the FBI investigators apprehended the administrator of Playpen and took control of the website. (*Id.* ¶ 30.) The agents then planned to allow the website to operate for a limited period of time to identify users of the website and to locate and rescue children from ongoing abuse. (*Id.*)

II. THE NETWORK INVESTIGATIVE TECHNIQUE WARRANT

On February 20, 2015, FBI investigators submitted an application for a search warrant, supporting attachments, and FBI Special Agent Douglas Macfarlane’s affidavit to the Authorizing Judge sitting in the Eastern District of Virginia. (Gov’t’s Resp., Ex. 1 at 2-35.) Agent Macfarlane’s affidavit explained that the FBI sought to use a network investigative technique (“NIT”) to identify Playpen users, which the FBI considered necessary due to the “unique nature of the Tor network” and because other investigative procedures were unsuccessful. (Macfarlane Aff. ¶¶ 31-32.) Under the NIT, the FBI would augment Playpen’s web content with instructions, so that once an activating

computer would log in and download Playpen’s web content, the instructions would cause the activating computer to send specific location-identifying information back to the government. (*Id.* ¶ 33.) Agent Macfarlane also explained that the FBI had moved a copy of the Playpen server, which contained the Playpen website contents, to a server at a government facility in the Eastern District of Virginia (*id.* ¶ 28) where the NIT would then “be deployed on [Playpen], while [Playpen] operates in the Eastern District of Virginia” (*id.* ¶ 32).

The FBI presented a warrant application to the Authorizing Judge, which stated that the government sought to search property described in “Attachment A” and seize property as described in “Attachment B.” (Gov’t’s Resp., Ex. 1 at 2, 34-35.) Attachment A provides that the NIT would be deployed on the seized computer server located in the Eastern District of Virginia to obtain information from “activating computers,” which are computers that log in Playpen by entering a username in password. (*Id.* at 34.) Attachment B provides the limited information that would be seized from activating computers. (*Id.* at 35.) It states that by operation of the NIT, an activating computer would send only the following: the computer’s IP address, the date and time the NIT determined the IP address, a unique identifier generated by the NIT to distinguish data from other activating computers, the type of operating system running on the computer, information about whether the NIT had already been delivered to the computer, and the computer’s host name, active operating system username, and medial access control address. (*Id.*)

On February 20, 2015, the Authorizing Judge approved the warrant application and issued a warrant (the “NIT Warrant”). (Gov’t’s Resp., Ex. 1 at 36-38.)

III. IDENTIFICATION OF CARLSON

The FBI deployed the NIT on Playpen between February 20, 2015, and March 4, 2015. (*Id.* at 40.) In February and March 2015, a Playpen user named “waytoco00l” accessed child pornography posts on Playpen’s website. (Gov’t’s Resp., Ex. 2 at 3-34 (“Moule Aff.”), ¶¶ 31-40.) According to data obtained from the NIT, the FBI ultimately determined that Carlson was the user “waytoco00l,” and on October 22, 2015, FBI Special Agent Glenn Moule obtained a warrant to search Carlson’s apartment in Minnesota (the “Second Warrant”). (Gov’t’s Resp. Ex. 2 at 2, 41; Moule Aff. ¶¶ 38-43.)

A. November 2015 Statements and Evidence

On November 2, 2015, FBI agents, in coordination with local police, executed the Second Warrant at Carlson’s apartment in Waseca, Minnesota. (Gov’t’s Resp., Ex. 2 at 41-45; Tr. of Mot. Hr’g at 8:12-16, 9:1-15, Feb. 13, 2017, Docket No. 33.) That morning, Agent Moule met Carlson in the front of his apartment building and explained the FBI had a warrant to search Carlson’s apartment. (Tr. of Mot. Hr’g at 12:20-22, 14:17-22.) After agents cleared the apartment, Agent Moule and another agent interviewed Carlson. (*Id.* at 16:19-20:8.)⁵ At one point during the interview, Carlson

⁵ Carlson was not handcuffed during the interview and moved freely about his residence. (Tr. of Mot. Hr’g at 27:9-20.) Roughly an hour into the interview – which began in Carlson’s apartment – Carlson requested moving to a local park, where the FBI continued the interview for about another hour. (*Id.* at 20:6-22, 22:9-13.)

stated that he was fascinated by child pornography. (*Id.* at 33:17-23.) During the search of Carlson's apartment, agents seized electronic devices; a subsequent forensic exam revealed that Carlson used his desktop computer to access child pornography on Playpen and that Carlson produced and distributed child pornography. (*Id.* at 35:5-36:18.)

B. November 2016 Statements

A year later, on November 17, 2016, Agent Moule executed another warrant (the "Third Warrant"), which authorized Carlson's arrest and a search of his person and residence, which was located at that time in Coleraine, Minnesota. (*Id.* at 8:17-21, 37:6-21, 38:20-22.) After Agent Moule arrested Carlson, Agent Moule and another FBI agent interviewed Carlson at the Coleraine Police Department. (*Id.* at 38:6-39:15.) Before the interview began, Carlson signed an Advice of Rights form, acknowledging that he understood and waived his *Miranda* rights. (*Id.* at 40:3-22.) During the course of the interview, Carlson confessed to producing child pornography. (*Id.* at 43:24-44:2.)

IV. PROCEDURAL BACKGROUND

On November 16, 2016, Carlson was charged with five counts of production of child pornography, in violation of 28 U.S.C § 2251(a) and (e); four counts of distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); and one count of possession of child pornography, in violation of U.S.C. § 2252(a)(4)(B) and (b)(2). (Indictment, Nov. 16, 2016, Docket No. 1.)

On January 17, 2017, Carlson moved to suppress all statements made to law enforcement with regard to the subject matter of this case and all evidence seized as a result of the NIT Warrant, including evidence seized during execution of the Second and Third Warrants. (Def.’s Mot. to Suppress Statements, Jan. 17, 2017, Docket No. 22; Def.’s Mot. to Suppress Evidence, Jan. 17, 2017, Docket No. 23.)

On March 23, 2017, the Magistrate Judge issued an R&R recommending that the Court grant Carlson’s motion to suppress evidence obtained as a result of the FBI investigation, grant Carlson’s motion to suppress as to his November 2015 statement to the FBI, and deny Carlson’s motion to suppress as to his November 2016 statement to the FBI. (R&R at 41, Mar. 23, 2017, Docket No. 44.) The Magistrate Judge reasoned that because the NIT Warrant was void, all evidence derived from it should be suppressed as fruits of an invalid warrant. (*Id.* at 22.) Accordingly, the Magistrate Judge recommended that the Court suppress Carlson’s November 2015 statement to the FBI. (*Id.* at 36-37.) However, because the Magistrate Judge determined that Carlson’s November 2016 statement was “sufficiently a product of [Carlson’s] free will to purge the taint of the NIT [W]arrant’s . . . [defects],” he recommended that the Court not suppress that statement. (*Id.* at 40-41.)

On April 24, 2017, the government filed several objections to the R&R. In response, Carlson asks the Court to adopt the R&R in its entirety. On July 24, 2017, the Eighth Circuit issued the decision in *Horton*, which involved the same NIT Warrant at issue here and implicated defendants whose activating computers were located in Iowa. 2017 WL 3122073. The *Horton* court reversed the District Court for the Southern

District of Iowa's ruling that ordered suppression of evidence obtained pursuant to the NIT Warrant, and held that the *Leon* good-faith exception to the exclusionary rule to evidence applied.

DISCUSSION

I. STANDARD OF REVIEW

After a magistrate judge files an R&R, "a party may serve and file specific written objections to the proposed findings and recommendations." Fed. R. Crim. P. 59(b)(2). For a dispositive matter such as a motion to suppress evidence, "[t]he district judge must consider *de novo* any objection to the magistrate judge's recommendation." Fed. R. Crim. P. 59(b)(1), (3); *see also* 28 U.S.C. § 636(b)(1). "The objections should specify the portions of the magistrate judge's [R&R] to which objections are made and provide a basis for those objections." *United States v. Pearson*, No. 15-117, 2015 WL 6445439, at *1 (D. Minn. Oct. 23, 2015) (quoting *Mayer v. Walvatne*, No. 07-1958, 2008 WL 4527774, at *2 (D. Minn. Sept. 28, 2008)).

Because Carlson's motions to suppress statements and evidence are dispositive motions, the Court reviews the R&R *de novo* in light of the government's objections.

II. GOVERNMENT'S OBJECTIONS

As a threshold matter, the government does not challenge Carlson's position that the deployment of the NIT was a Fourth Amendment search. (*See* R&R at 10.) Furthermore, neither party objects to the R&R's recommendation not to suppress Carlson's November 2016 statement. The government objects to the R&R's

recommendation that the Court suppress all evidence derived from the NIT Warrant and Carlson's November 2015 statement. More specifically, the government objects to the Magistrate Judge's conclusions that: (1) the NIT Warrant lacked particularity; (2) the NIT Warrant violated the Fed. R. Crim. P. 41(b); (3) all evidence derived from a purported Rule 41 violation requires suppression; (4) the *Leon* good-faith exception does not apply in this case. (*Id.* at 10-37.) The Court will address each of the government's objections in turn.

A. Constitutional Issues

The government first objects to the Magistrate Judge's conclusion that the NIT Warrant was constitutionally deficient because it "fail[ed] to particularly describe the place to be searched." (*Id.* at 23.)⁶

A warrant is valid for purposes of the Fourth Amendment if it is (1) issued by a neutral and detached magistrate, (2) supported by probable cause, and (3) sufficiently particular in its description of the "things to be seized" and the "place to be searched." *Dalia v. United States*, 441 U.S. 238, 255 (1979); *United States v. Faulkner*, 826 F.3d 1139, 1145-46 (8th Cir. 2016).⁷ A warrant is sufficiently particular if "the items to be seized and the places to be searched [are] described with sufficient particularity as to

⁶ As the Magistrate Judge acknowledged, "every other court to consider the question of particularity under the facts of this case has concluded that the NIT [W]arrant was sufficiently particular." (R&R at 23 n.9.) In addition, the *Horton* court declined to address whether the NIT Warrant met the Fourth Amendment's particularity requirement. 2017 WL 3122073, at *4 n.3.

⁷ The Fourth Amendment requires that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

enable the searcher to locate and identify the places and items with reasonable effort and to avoid mistakenly searching the wrong places or seizing the wrong items.” *United States v. Gleich*, 397 F.3d 608, 611 (8th Cir. 2005).

The Magistrate Judge found that the NIT Warrant and Attachment A (which described the place to be searched) “do[] not identify which computers will be searched until the search is actually completed” (R&R at 24) and “it is not possible to identify with any specificity, which computers, out of all of the computers on earth, might be searched pursuant to this warrant” (R&R at 23). The Court disagrees with the R&R’s interpretation of the NIT Warrant. Attachment A sufficiently described the “place to be searched” as any activating computer that logged in to Playpen with a username and password, not simply any computer on earth. (See Gov’t’s Resp., Ex. 1 at 37.) The NIT Warrant also limited what information could be obtained as a result of the search and when the search would occur. (See Gov’t’s Resp., Ex. 1 at 36-40.) Courts often permit an anticipatory search warrant where the existence of probable cause is dependent upon the occurrence of some triggering condition precedent. *United States v. Grubbs*, 547 U.S. 90, 95 (2006). Carlson does not dispute that there was probable cause supporting the NIT Warrant, and the triggering condition precedent here was that he accessed Playpen, which then authorized deployment of the NIT on his activating computer.

Moreover, the purpose of the NIT Warrant was to learn the location of anonymous computers accessing Playpen. “[W]hether a warrant fails the particularity requirement cannot be decided in a vacuum. The [C]ourt will base its determination on such factors as the purpose for which the warrant was issued, the nature of the items to which it is

directed, and the total circumstances surrounding the case.” *Milliman v. Minnesota*, 774 F.2d 247, 250 (8th Cir. 1985) (citation omitted). Agent Macfarlane explained that the NIT was necessary as “other investigative procedures that are usually employed in criminal investigations of this type ha[d] been tried and ha[d] failed or reasonably appear[ed] to be unlikely to succeed if . . . tried.” (Macfarlane Aff. ¶ 31.) That the NIT Warrant had the possibility of ensnaring a large number of users logging into the Playpen site does not mean it lacked particularity.

Finally, the NIT Warrant did not limit itself to searches in the Eastern District of Virginia. Although the NIT Warrant granted the government the ability to search property “located in the Eastern District of Virginia,” it also specified that the “property to be searched” was found in Attachment A. (Gov’t’s Resp., Ex. 1 at 36.) In turn, Attachment A explained that the server “operating the Tor network child pornography website” would be “located at a government facility in the Eastern District of Virginia,” and that the government would “deploy[]” the NIT on the server to obtain “information . . . from the activating computers,” which are computers that belong to “any user or administrator who logs into the TARGET WEBSITE by entering a username and password.” (Govt’s Resp., Ex. 1 at 37.) Thus, reading the NIT Warrant as a whole – which expressly incorporates the Attachments – it is clear that the “place to be searched” was any activating computer that accessed Playpen, and the warrant was requested in the Eastern District of Virginia because the government would install and operate the server there. (Gov’t’s Resp., Ex. 1 at 36-40.) This is entirely consistent with the NIT Warrant

application, attachments, and Agent Macfarlane’s supporting affidavit. (See Gov’t’s Resp., Ex. 1 at 2-35.)

Thus, as the Court finds the NIT Warrant was sufficiently particular, it will reject the R&R and sustain the government’s objection on this ground.

B. Authority Under Rule 41(b)(4)

The government next objects to the Magistrate Judge’s conclusion that the geographic reach of the NIT Warrant exceeded the Authorizing Judge’s territorial jurisdiction.

The Federal Magistrate Judge Act provides that a magistrate judge within his or her district has “all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts.” 28 U.S.C § 636(a)(1). In turn, Fed. R. Crim. P. 41(b) (2015) enumerates circumstances when a magistrate judge may issue a warrant.⁸ At issue here is whether Rule 41(b)(4) permitted the Authorizing Judge to issue the NIT Warrant. Rule 41(b)(4) provides that “a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both.” A “tracking device” is defined as “an electronic or mechanical device which permits the tracking of the movement of a

⁸ On December 1, 2016, the Federal Rules of Criminal Procedure were amended to provide an additional circumstance where a magistrate judge may issue a warrant for situations that may involve a NIT. *See* Rule 41(b)(6).

person or object.” Fed. R. Crim. P. 41(a)(2)(E) (incorporating the definition set out in 18 U.S.C. § 3117(b)).

The government objects to the conclusion reached in the R&R that the NIT was not a valid tracking device under Rule 41(b)(4). In *Horton*, the Eighth Circuit considered the same issue, and rejected the government’s argument that for purposes of Rule 41(b)(4), the NIT was “installed” within the Eastern District of Virginia when Playpen users made a virtual trip to that district. 2017 WL 3122073, at *3. Instead, the court held that the NIT “installed” on each activating computer wherever located, and because the activating computers in *Horton* were located in Iowa, the Authorizing Judge exceeded her jurisdiction under Rule 41(b)(4). *Id.* Applying that line of reasoning, because Carlson’s activating computer was located in Minnesota, the NIT Warrant also fails to be a valid tracking device under Rule 41(b)(4) because the device was installed in Minnesota rather than the Eastern District of Virginia. Thus, consistent with determination reached in the R&R and *Horton*, the Court finds that the NIT warrant exceeded the Authorizing Judge’s jurisdiction.

C. Exclusion of Evidence Based on Rule 41(b) Violation

The government next objects to the Magistrate Judge’s conclusion that the Rule 41(b) violation amounts to a constitutional error, which presumably triggers the exclusionary rule to evidence.

Even though the NIT Warrant did not comply with Rule 41(b), “[n]oncompliance with [Rule] 41 prerequisites does not automatically require the exclusion of evidence in a

federal prosecution.” *United States v. Schoenheit*, 856 F.2d 74, 76 (8th Cir. 1988). “Absent a constitutional infirmity, the exclusionary rule is applied only to violations of [Rule] 41 that prejudice a defendant or show reckless disregard of proper procedure.” *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993); *see also United States v. Welch*, 811 F.3d 275, 280 (8th Cir. 2016) (“[A Rule 41] procedural violation is not per se an unreasonable search and seizure in violation of the Fourth Amendment.”). As previously stated, a warrant is valid for purposes of the Fourth Amendment if, among other requirements, it is issued by a neutral and detached magistrate. *Dalia*, 441 U.S. 238, 255 (1979).

“[I]nherent in the notion of a ‘neutral, detached magistrate’ is that the magistrate have authority to issue the warrant.” *Horton*, 2017 WL 3122073, at *4 (quoting *United States v. Taylor*, No. 16-203, 2017 WL 1437511, at *14 (N.D. Ala. Apr. 24, 2017)). Because the Authorizing Judge lacked jurisdiction, and thus authority, to issue the NIT Warrant, there was no judicial approval of the NIT Warrant as required by the Fourth Amendment. *Horton*, 2017 WL 3122073, at *4. Thus, consistent with determination reached in the R&R and in *Horton*, the Court finds the Rule 41(b) violation was of constitutional magnitude, and that the exclusionary rule to evidence obtained as a result of the NIT Warrant presumably applies, barring an exception.⁹

⁹ Because a warrant issued outside of the Authorizing Judge’s jurisdiction is a constitutional error, the Court need not address prejudice or reckless disregard for procedure. *Hyten*, 5 F.3d at 1157; *Horton*, 2017 WL 3122073, at *4.

D. Good Faith

The government lastly objects to the R&R's conclusion that the *Leon* good-faith exception to the exclusionary rule does not apply to this case. In *United States v. Leon*, the Supreme Court established an "objective good faith" exception to the exclusionary rule and held that evidence obtained pursuant to a warrant later determined to be invalid under the Fourth Amendment is admissible if the executing officer's reliance on the issued warrant, and belief that the issued warrant was valid, were reasonable. 468 U.S. 897, 921-24 (1984).

Here, the *Leon* exception applies because there is nothing in the record to imply that the FBI relied on the NIT Warrant unreasonably or in bad faith. *Id.*; *Horton*, 2017 WL 3122073, at *5.¹⁰

"The [*Leon*] good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization." *United States v. Clay*, 646 F.3d 1124, 1127 (8th Cir. 2011) (quoting *United States v. Perry*, 531 F.3d 662, 665 (8th Cir. 2008)). In this case, the jurisdictional error was made by a magistrate judge, not the FBI. The

¹⁰ The Eighth Circuit rejected the R&R's conclusion that *Leon* is inapplicable,` a warrant void *ab initio*, and held that the *Leon* good-faith inquiry does not depend on the type of Fourth Amendment violation but instead on whether the police acted with good-faith. *Horton*, 2017 WL 3122073, at *5. The good-faith exception requires a "rigorous weighing of [the exclusionary rule's] costs and deterrence benefits," and "[t]he basic insight of the *Leon* line of cases is that the deterrence benefits of exclusion 'var[y] with the culpability of the law enforcement conduct' at issue." *Davis v. United States*, 564 U.S. 229, 238 (2011) (quoting *Herring v. United States*, 555 U.S. 135, 143 (2009)). Accordingly, the focus of the good-faith exception does not depend on whether the Rule 41 violation is substantive or technical, but rather, whether police misconduct outweighs the benefit of admitting evidence.

Supreme Court has consistently expressed a “strong preference for warrants” and mandated “great deference” to a magistrate’s determination that a warrant is constitutionally sufficient. *Leon*, 468 U.S. at 914 (citation omitted).

Here, it was reasonable for the agents to have deferred to and relied on the Authorizing Judge’s determination of her territorial authority to issue the NIT Warrant. *See Leon*, 468 U.S. at 921 (“In the ordinary case, an officer cannot be expected to question the magistrate’s . . . judgment that the form of the warrant is technically sufficient.”); *United States v. Houston*, 665 F.3d 991, 996 (8th Cir. 2012) (declining to “impose” on an officer the “duty” of ascertaining the “legal and jurisdictional limits of a judge’s power to issue interstate search warrants”). Additionally, there is no evidence suggesting that Agent Macfarlane had insight or knowledge regarding the nuances of Rule 41(b) to suggest that he intentionally or deliberately disregarded that rule. Moreover, the fact that numerous other district courts have held that Rule 41(b)(4) authorized the NIT Warrant suggests his actions were reasonable.

Finally, the uncontested record supports that the FBI acted in good faith and generally followed proper procedures in requesting and executing the NIT Warrant. The FBI devised the NIT to track anonymous Playpen users; described the NIT’s process and utility in a warrant application, attachments, and detailed affidavit; presented those documents to a magistrate judge in the district where the server housing the website was located and the NIT would be deployed; obtained judicial authorization for the search; and executed the NIT according to the warrant’s terms.

Thus, consistent with the holding in *Horton*, which is binding on this Court, the Court finds that even though the Rule 41(b) violation rose to the level of a Fourth Amendment violation, there was no FBI misconduct to outweigh the cost of suppressing the evidence under the *Leon* good-faith test. *See* 2017 WL 3122073, at *5-7 (holding same). Therefore, the Court will sustain the government's objections to the R&R and deny Carlson's motions to suppress evidence and statements obtained by the FBI as a result of the NIT Warrant.

ORDER

Based on the foregoing, and all the files, records, and proceedings herein, the Court **SUSTAINS** the United States' Objections [Docket No. 51] and **ADOPTS in part** and **REJECTS in part** the Report & Recommendation of the Magistrate Judge [Docket No. 44]. Accordingly, **IT IS HEREBY ORDERED** that:

1. The Report & Recommendation [Docket No. 44] is **REJECTED** to the extent that it recommends granting Defendant Terry Lee Carlson, Sr.'s motions to suppress. In all other respects, the Report & Recommendation [Docket No. 44] is **ADOPTED**.
2. Defendant's Motion to Suppress Statements [Docket No. 22] is **DENIED**.
3. Defendant's Motion to Suppress Evidence obtained as a Result of Search and Seizure [Docket No. 23] is **DENIED**.

DATED: August 7, 2017
at Minneapolis, Minnesota.

s/John R. Tunheim
JOHN R. TUNHEIM
Chief Judge
United States District Court